SJR 38 Victim Assistance & Other ID Theft Bill Draft Explanations

Bill#	Section#	Provisions
8877 Victim assistance (salmon)	Section 1	1) Provides that 2 forms of ID to be provided to determine ID of victim, including driver's license or other photo ID, utility bill *(list of items similar to those used to register to vote).* 2) Law enforcement to provide one copy to victim, another copy to attorney general for ID theft passport. 3) Requires law enforcement to take complaint even if crime happened elsewhere. Allows referral to law enforcement where jurisdiction is suspected. 4) Requires cooperation with other law enforcement and investigation within its resources. Doesn't require cases to be listed for statistics.
	Section 2	Consumer access to information. Uses definition of information broker from HR 4127, a bill draft before Congress.
	Section 3	Revises existing law to allow person who is a resident of Montana to file for an ID theft passport, even if victimized elsewhere. Allows resident victimized elsewhere to apply directly to Department of Justice for ID theft passport, instead of going through law enforcement agency. Allows copy of police report or other "substantial evidence of having filed a complaint". ***WA law: 9.35.020(5) In a proceeding under this section, the crime will be considered to have been committed in any locality where the person whose means of identification or financial information was appropriated resides, or in which any part of the offense took place, regardless of whether the defendant was ever actually in that locality.***

	Section 4	1) Victim may apply to court to expunge victim's own record if there are entries recorded because another person assumed the victims identity and that person was convicted of crimes (but using the victim's name). 2) Requires ID theft passport and other documents to establish that convicted person was actually someone else. 3) Court to send copy of expungement order to Department of Justice and department to expunge its relevant records. 4) Requires insurance company to refund the additional premium charged because of a conviction upon expungement of record and notification of the expungement. 5) Prohibits fee for court costs. 6) (misnumbered) Gives rulemaking authority to Department of Justice. ***WA law: 9.35.020(7) In a proceeding under this section in which a person's means of identification or financial information was used without that person's authorization, and when there has been a conviction, the sentencing court may issue such orders as are necessary to correct a public record that contains false information resulting from a violation of this section.***
	Section 5.	1) Requires block of information by consumer reporting agency that resulted from identity theft. 2) Sets out consumer's process for requesting a block of information. 3) Consumer reporting agency to provide information furnisher (3rd party) that police report has been filed, block is requested, and effective date of block. 4) Allows consumer reporting agency not to block, for misrepresented facts, error, consumer's knowing possession of goods, etc. as result of blocked transaction. 5) Process for letting consumer know if information not to be blocked. 6) Requires law enforcement to provide copy of police report to consumer for use in blocking information. ***Washington has a block of information provision in RCW 19.182.160.***
	Section 6	Codification in Title 46, chapter 24, part 2 - Services to Victim, Witness
	What's missing	• Provision prohibiting collecting agencies from calling ID theft victims multiple times once they have been notified that a series of checks have been misappropriated or stolen. • Provisions enhancing criminal penalties • Provisions requiring entities to notify individual if the entity knows that an individual's ID is being misused. Apparently financial institutions are not allowed to address this by federal statute. SSA has an Advocate Program that can help track multiple uses of a person's Social Security number. However, most state agencies that use SSNs do not verify the accuracy of the number - a process that costs money. Motor Vehicle Division/Secretary of State verify numbers.
Bill#	**Section#**	**Provisions**

8800 expands to agencies notice provision of computer security breach (orange)	Section 1.	Expands definitions in existing law to include agencies -- all branches of state government and county, city or other political subdivision of the state. NJ & WA have state notification **(WA law--*RCW 42.17.31922*--includes: *An agency shall not be required to disclose a technical breach of the security system that does not seem reasonably likely to subject customers to a risk of criminal activity.)***
	Section 2.	Includes reference to public record retention/disposal requirements for agencies.
	Section 3.	Adds agencies to breach notification in existing law (which addresses business).
	Section 4.	1) Gives the Lewis and Clark County Attorney responsibility for pursuing complaint against Department of Justice if a security breach affects DOJ. Repeats procedure for Lewis and Clark County Attorney that Attorney General has for others. 2) Distinguishes between violations by business or person, which is covered under 30-14-103 (unfair methods of competition, or deception in trade or commerce). Penalties under 30-14-142 are up to $10,000 civil fine for violating injunction or temporary restraining order. Willful use of an unfair practice may result in fine of up to $10,000, which is in addition to liability for violating injunction. 3) Subsection 3(b) says agency may be required to pay for a credit report in security breach. ***(Does not say by whom. This payment is not required for businesses.)*** Also allows court to assess cost of action. Gives waiver to Lewis and Clark County Attorney if action brought against DOJ and violation did not occur. 4) Subsection (3)(c) allows agency to take disciplinary action against a state employee for failing to notify of breach. ***(Does not say about other employees).***
Bill#	**Section#**	**Provisions**

8899 written approval required for transport of hardware or software outside state campus (blue)	Section 1.	1) Prohibits public officers and those under contract with a public agency from taking hardware or software with unencrypted information outside a public building without written authorization. 2) Restricts access through statewide telecommunications network by contractor or public officer to another individual's personal information without written authorization from individual and -- for public employee -- authorization by employee's supervisor. Statewide telecommunications network is defined in 2-17-506 (9) as: "any telecommunications facilities, circuits, equipment, software, and associated contracted services administered by the department for the transmission of voice, video, or electronic data from one device to another." 3) Restricts access to full data fields if teleworking. 4) Requires secure connections for access. 5) Limits storage of data if accessed from statewide telecommunications network unless access device provided by public agency and updated for security purposes. 6) Applies to National Guard and all branches of state government.
	Section 2.	Violation is official misconduct. 45-7-401 requires fine of up to $500, or up to 6 months in county jail or both.
	Section 3.	Codification in Government Structure & Administration, Information Technology - Internet Privacy section
	Section 4.	Immediate effective date

	Comment	Discussions in the work group indicated the Department of Administration's Information Technology Services Division (ITSD) might move forward with a policy for state employees. The Division's policy would not cover all state employees. Excluded are legislative and judicial branch employees plus National Guard employees. Because not all agencies are covered, a bill draft was developed to address issues more broadly. Policy option includes whether to let ITSD policy stand or make it broader. Provisions of the interim data security policy approved by ITSD on July 7, 2006 include: 1) use of portable devices and electronic storage media on or off state premises; 2) supplements ENT-SEC-112, which does not apply to colleges, universities, Commissioner of Higher Education or public access computers in libraries; 3) restricts collection, storage and use of sensitive data (e.g. SSNs), and bases access on business requirements & management authorization; 4) prohibits copying or removal of sensitive data from secured storage environments.